УДК 343.98

А. В. Даниленко,
курсант 3-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Д. И. Шнейдерова,
старший преподаватель кафедры
уголовного права, уголовного процесса и криминалистики
Могилевского института МВД

КРИМИНАЛИСТИЧЕСКОЕ ЗНАЧЕНИЕ ДОПРОСА ПОТЕРПЕВШЕГО ПРИ ОБНАРУЖЕНИИ ЦИФРОВЫХ СЛЕДОВ

В условиях глобальной цифровизации наблюдается планомерное и набирающее обороты развитие кластера преступлений, в механизмах которых используются компьютерные технологии и сети. В этой связи актуальность и практическую значимость приобретают вопросы трансформации апробированных тактик проведения отдельных следственных действий под условия усовершенствованных механизмов киберпреступлений в целях разработки эффективных средств и алгоритмов обнаружения, фиксации и исследования цифровых следов. К одному из наиболее сложных с точки зрения тактики следственных действий сотрудники правоохранительных органов и ученые-криминалисты (Н. П. Яблоков, Е. С. Шевченко, Т. В. Радченко, Г. С. Девяткин, М. А. Киселева и иные) относят допрос по ряду причин, среди которых на первых позициях выступают следующие: отсутствие должного объема специальных знаний в сфере информационных технологий у сотрудников, осуществляющих предварительное расследование; незнание специфической терминологии и неумение ее применять при допросе; низкий уровень информационного обеспечения, позволяющего грамотно определить границы предмета допроса; недостаточность первичных сведений о способе совершенного преступления и его следовой картине.

Вместе с тем допрос, являясь одним из первоначальных следственных действий по уголовному делу, в частности допрос потерпевшего, позволяет получить сведения о способе совершенного преступления, о предмете преступного посягательства и его особенностях, характере и размере вреда, ориентирующую информацию об источниках цифровых следов, использованных программных и технических средствах (как потерпевшим, так и преступником), а также представление об уровне владения специальными знаниями в сфере IT допрашиваемым, что в совокупности окажет непосредственное влияние на дальнейший ход расследования и поможет определиться с перечнем необходимых следственных и процессуальных действий в правильной последовательности их реализации.

Как показывает сложившаяся правоохранительная практика, на первоначальном этапе расследования киберпреступлений проблематично установить информационную целостность механизма совершенного преступления и определить, какие же цифровые следы подлежат отысканию. В этом случае криминалистическую значимость приобретают результаты допроса потерпевшего, который в своих показаниях ориентирует следователя на источники доказательственной информации, подлежащие первостепенному исследованию, например, какие следует осмотреть веб-ресурсы (фишинговые и иные сайты, аккаунты в социальных сетях, объявления на торговых площадках, форумы, кабинеты крипто- и электронных кошельков, интернет-банкинга, электронную почту и т. д.), компьютерные и мобильные устройства, съемные носители цифровых данных, программы и приложения, задействованные в преступлении, в какие организации направить запросы для получения справочной и доказательственной информации, каких специалистов привлечь для участия в следственных действиях и консультирования.

При этом результативность дальнейших действий, как и полнота информации, получаемой при допросе, зависит, по мнению Н. П. Яблокова, от должного уровня знаний компьютерных и интернет-технологий, позволяющих следователям разобраться в способах действий преступников по следовой картине киберпреступлений [1, с. 374]. Поскольку квалификация правоохранителей не предполагает наличия технического образования, то получают такие знания они преимущественно за счет самостоятельного изучения общедоступных литературных и сетевых источников, на поиск и освоение которых затрачивается большое количество времени, к тому же, если рассматривать ресурсы сети Интернет, то достоверность приводимой в них информации нередко вызывает сомнения. Кроме того, изучение теоретической основы еще не свидетельствует о выработке навыков грамотного ее применения при допросе. В некоторых случаях уровень владения компьютерными технологиями потерпевшим базовый, и, чтобы получить от него интересующую информацию, лицу, производящему допрос, необходимо правильно формулировать вопросы, а в отдельных случаях и разъяснять технологию отдельных информационных процессов, чтобы потерпевший осознал, какие сведения от него хотят получить. Не исключается и противоположная ситуация, когда следователь, получив от «технически продвинутого» потерпевшего некоторую информацию, не сможет определить ее значимость и относимость к делу, тем самым не обратив на нее должного внимания.

Таким образом, допрос потерпевшего на первоначальном этапе расследования киберпреступлений является центральным источником сведений, ориентирующих следствие на обнаружение источников цифровых следов. И поскольку во многом результативность допроса зависит от подготовки следователя

к его проведению, в частности, от уровня, полноты и качества информационного обеспечения, то представляется целесообразной разработка межведомственного цифрового справочного комплекса для правоохранительных органов, содержащего необходимый периодически обновляемый комплекс достоверной информации о технических особенностях функционирования компьютерных и сетевых ресурсов, используемых в преступных механизмах, образуемых при этом цифровых следах, с указанием контактных данных специалистов, способных оказать консультационное содействие при возникновении вопросов.

1. Яблоков Н. П. О некоторых особенностях криминалистической тактики расследования преступлений в условиях цифрового мира // Енисейские политико-правовые чт. : сб. ст. / Краснояр. регион. обществ. орг. «Общественный комитет по защите прав человека» ; отв. ред.: Г. Л. Москалев, Е. А. Акунченко. Красноярск, 2019. С. 372–379. Вернуться к статье